A CLASS OF FINITE COMPUTATION STRUCTURES SUPPORTING THE FAST FOURIER TRANSFORM

Richard J. Bonneau

Massachusetts Institute of Technology

Prepared for:

Office of Naval Research
Advanced Research Projects Agency
National Science Foundation

March 1973

UNCLASSIFIED
Security Classification

AD-757 787

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY *(Corporate author)*
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
PROJECT MAC

2a. REPORT SECURITY CLASSIFICATION
UNCLASSIFIED

2b. GROUP
NONE

3. REPORT TITLE
A CLASS OF FINITE COMPUTATION STRUCTURES SUPPORTING THE FAST FOURIER TRANSFORM

4. DESCRIPTIVE NOTES *(Type of report and inclusive dates)*
INTERIM SCIENTIFIC REPORT

5. AUTHOR(S) *(First name, middle initial, last name)*
RICHARD J. BONNEAU

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
MARCH, 1973	15	12

8a. CONTRACT OR GRANT NO.	9a. ORIGINATOR'S REPORT NUMBER(S)
N00014-70-A-0362-0006	
b. PROJECT NO.	
c.	9b. OTHER REPORT NO(S) *(Any other numbers that may be assigned this report)*
d.	NONE

10. DISTRIBUTION STATEMENT
DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY
	OFFICE OF NAVAL RESEARCH

13. ABSTRACT

The Fast Fourier Transform (FFT) and modular arithmetic are two distinct techniques which recently have been employed to increase the efficiency of numerous algorithm in the area of symbolic and algebraic manipulation. Motivated by work done on fast large integer multiplication by Schonhage and Strassen [11] and by Knuth [7], this paper analyzes the question of when these two techniques can be utilized concurrently. The desirability of the convolution property of the FFT suggests a practical definition for the support of an FFT, while a generalization of the modular rings of integers motivates a resonable definition of a finite computation structure. A Finite Computation Structure is defined to be a commutative ring with unity, and of finite, non-zero charater-istic. This report first completely characterizes the modular rings of integers which support the FFT by considering the prime factorization of the modulus. This result: Theorem: Let R be a finite computation structure of characterization m. Then R will support a K-point FFT if K divides p-1 for each prime p dividing m. The paper then concludes with examples of the application of this result to the problems of computing products and powers of symbolic multivariate polynomials.

DD FORM 1 NOV 68 1473 (PAGE 1)
S/N 0102-014-6600

UNCLASSIFIED
Security Classification

17

14 KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Fast Fourier Transform						
Finite Computation Structures						
Modular arithmentic						
Symbolic polynomial manipulation						

A CLASS OF FINITE COMPUTATION STRUCTURES SUPPORTING THE FAST FOURIER TRANSFORM

Richard J. Bonneau

MAC Technical Memorandum 31

March 1973

Work reported here is supported in part by the Raytheon Advanced Degree Program and by Project MAC, an M.I.T. research program sponsored by the Advanced Research Projects Agency, Department of Defense, under ARPA Order No. 2095 and under Office of Naval Research Contract Number N00014-70- A-0362-0006 and the National Science Foundation under contract number GJ00-4327.

Massachusetts Institute of Technology

PROJECT MAC

Cambridge Massachusetts 02139

Section 1. Introduction

The Fast Fourier Transform (FFT) and modular arithmetic are two distinct techniques which recently have been employed to increase the efficiency of numerous algorithms in the area of symbolic and algebraic manipulation. Motivated by work done on fast large integer multiplication by Schönhage and Strassen [11] and by Knuth [7], this paper analyzes the question of when these two techniques can be utilized concurrently. The desirability of the convolution property of the FFT suggests a practical definition for the support of an FFT, while a generalization of the modular rings of integers motivates a reasonable definition of a finite computation structure. A Finite Computation Structure is defined to be a commutative ring with unity, and of finite, non-zero characteristic. This report first completely characterizes the modular rings of integers which support the FFT by considering the prime factorization of the modulus. This characterization is then extended to provide the following result: Theorem: Let R be a finite computation structure of characteristic m. Then R will support a K-point FFT if K divides p-1 for each prime p dividing m. The paper then concludes with examples of the application of this result to the problems of computing products and powers of symbolic multivariate polynomials.

Section 2. The Discrete Fourier Transform

Definition: Let R be a commutative ring with unity, written as 1, K an integer > 1, and WK an element of R of order K; i.e., a primitive K-th root of unity. Then the DISCRETE FOURIER TRANSFORM (DFT) of the K-sequence (a0,a1,.. .,a(K-1)) is the K-sequence

$$(\hat{a}0,\hat{a}1,\ldots,\hat{a}(K-1))$$

given by the following equations:

$$\hat{a}_j = \sum_{i=0}^{K-1} a_i W_K^{ij} \qquad 0 \le j \le K-1 \qquad (1)$$

Definition: Assuming the same conditions as above, and also, that K possesses a multiplicative inverse in R (i.e. 1/K), then the INVERSE DISCRETE FOURIER TRANSFORM (IDFT) of the K-sequence (a0,a1,...,a(K-1)) is the K-sequence

$$(\hat{a}0,\hat{a}1,\ldots,\hat{a}(K-1))$$

given by the following equations:

$$\hat{a}_j = (1/K) \sum_{i=0}^{K-1} a_i W_K^{-ij} \qquad 0 \le j \le K-1 \qquad (2)$$

If we consider the term ai*WK**(-i*j) to be rewritten as the equivalent term

$$ai*WK**((K-i)*j)$$

then we can rewrite the above equation as

$$\hat{a}_j = (1/K) \sum_{i=0}^{K-1} a_{K-i} W_K^{ij} \qquad (2a)$$

If we now define a(K) = a(0), then the inverse DFT can be computed from the DFT by merely "flipping" the input sequence. Here, flipping consists in replacing the i-th term by the (K-i)-th term. Thus the same computational algorithm (for the DFT) can be used to compute both the DFT and the IDFT. As might be expected from the terminology, under the right conditions, the two transforms are inverses of each other, and thus provide different representations of K-sequences. The remainder of this paper will be concerned with determining some of the "right" conditions under which the DFT can be inverted. Note, also, that the DFT (and the IDFT) are linear transformations from R**K to R**K, (where R**K is the ring of K-tuples of elements of R with component addition and multiplication) since the quantities WK**(i*j) are all "constants" for each application of the DFT. For more information on this approach to the phenomenon of the DFT, see Nicholson [10].

The computation of the DFT by classical techniques usually involved O(K**2) operations, as the computation of each

transformed element took K multiplications followed by K-1 additions. However, Cooley and Tukey [5] demonstrated a computation scheme by which the DFT of a K-sequence could be computed in only O(K log K) operations. This method has become known as the Fast Fourier Transform (FFT). The key concept in the reduction of the computation time involves the factorization of K. In other words, for K highly composite, the DFT can be computed by forming sub-sequences of the original sequence, performing a DFT of fewer elements on them, then assembling the resulting sequences. The goal here is not to develop the theory surrounding the FFT (see Cooley-Tukey [5]) but rather to instill some feeling for the immense efficiency of this algorithm and thus to motivate the desire to find as many ways as possible in which it can be invoked. During the remainder of this paper, the terms DFT and FFT will be used interchangeably, as they refer to a computation function and a computation algorithm which correspond to each other.

The particular virtue of the DFT in many applications results from the following:

Definition: Let A = (a0,a1,.. .,a(K-1)) and B = (b0,b1,.. .,b(K-1)) be two K-sequences in R. Then the CONVOLUTION OF A AND B, written A*B, is the K-sequence C = (c0,c1,.. .,c(K-1)) where the cj are defined as follows:

$$c_j = \sum_{i=0}^{K-1} a_i \, b_{j-i} \qquad 0 \le j \le K-1 \qquad (3)$$

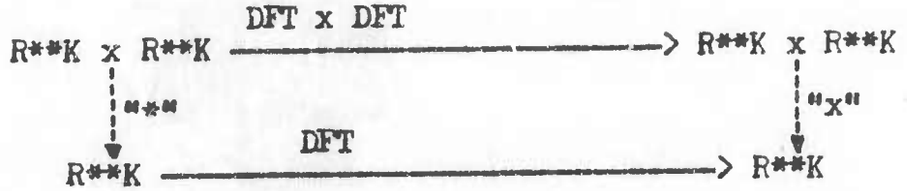
where bn for n < 0 is defined as b(n+K).

Convolution Property of the DFT:

Let A and B be as in the preceding definition. Let A' and B' be the DFT's of A and B respectively. Then the following equation is true:

$$(A*B)' = A' \times B' \qquad (4)$$

where "x" means component-wise multiplication of K-sequences. In other words, the DFT transforms the convolution operation in R**K into the component-multiplication in R**K, according to the following commutative diagram:



Proof:

$$\hat{c}_l = \sum_{j=0}^{K-1} c_j \omega_K^{jl} = \sum_{j=0}^{K-1} \sum_{i=0}^{K-1} a_i b_{j-i} \omega_K^{jl}$$

$$= \sum_{j=0}^{K-1} \sum_{i=0}^{K-1} a_i b_{j-i} \omega_K^{(j-i)l} \omega_K^{il}$$

$$= \sum_{i=0}^{K-1} a_i \omega_K^{il} \underbrace{\left(\sum_{j=0}^{K-1} b_{j-i} \omega_K^{(j-i)l} \right)}$$

$$= \sum_{i=0}^{K-1} a_i \omega_K^{il} \hat{b}_l$$

$$= \hat{a}_l \cdot \hat{b}_l$$

QED.

As a result of (4), the convolution of two K-sequences can be computed in the following way:

1) compute the transforms A′ and B′ of A and B respectively.
2) perform componentwise multiplication on A′ and B′ to obtain a K-sequence C′.
3) perform the inverse DFT on C′ to obtain the convolution sequence C.

Thus, the DFT provides a method (though not an intuitive one) for computing the convolution of sequences, assuming that the inverse DFT of step 3 is possible; i.e., if we can turn the bottom arrow around in the above figure. What this requirement amounts to is that we must able to compute a "true" inverse DFT.

Let us now look into the requirements for the invertibility of the DFT. If we apply the inverse DFT of equation 2 to the sequence of elements computed via the DFT of equation 1, the

following equations will hold:

$$\hat{\hat{a}}_l = \sum_{j=0}^{K-1} \hat{a}_j \omega_K^{-jl} = \frac{1}{K} \sum_{j=0}^{K-1} \sum_{i=0}^{K-1} a_i \omega_K^{j(i-l)} = \frac{1}{K} \sum_{i=0}^{K-1} a_i \sum_{j=0}^{K-1} \omega_K^{j(i-l)}$$

As a result, the IDFT, as defined originally, will be a true inverse <===> a"hat-hat sub 1" = a"sub 1" for all $1 \leq K-1$ <===>

$$\sum_{j=0}^{K-1} \omega_K^{j(i-l)} = K \cdot \delta_{0,i-l} \qquad 0 \leq i, l \leq K-1$$

(Recall that delta(i,j) = 1 if i=j and 0 otherwise.) Notation: Inasmuch as the following quantity appears quite frequently in the rest of this paper, we use the following notation:

$$S_l \triangleq \sum_{i=0}^{K-1} \omega_K^{il} \qquad 0 \leq l \leq K-1$$

Using this notation, we obtain the requirement: The IDFT is an inverse <===> S"sub 1" = K delta(0,1). Thus, a reasonable basis upon which to build a useful DFT (i.e., one able to produce the convolution) is to define:

Definition: Let K be > 1. The Support of a K-point DFT is a commutative ring R with identity such that

(S1) There exists 1/K in R.
(S2) There exists wK in R whose order = K.
(S3) S"sub 1" = K delta(0,1) for all $1 \leq K-1$.

Note that the support of an FFT is an "essential" property of a ring ; i.e., if a ring R supports a K-point FFT and R is contained in a larger ring R', then R' also supports K-point FFT's.

Two examples of support of a K-point DFT are the complex numbers with wK being the complex number $\cos(2\pi/K)+\sqrt{-1}\,\sin(2\pi/K)$, and also the algebraic number field Q[ξ], where ξ is a formal solution to the equation x**K = 1, and Q is the field of rational numbers.

Section 3. Finite Computation Structures

This section deals with the problem of developing a sufficiently rich generalization of the structure of modular rings of

integers. The motivation for this generalization derives from the desire to develop data structures whose underlying arithmetic is precisely modular arithmetic. This will enable the modelling of a data structure within a computer. As a result of this thinking, we propose the following:

Definition: A Finite Computation Structure is a commutative ring with unity, having finite, non-zero characteristic. (Recall that the characteristic of a ring is the smallest integer m such that ma = 0 for all a in the ring. See Lang [8] and Albert [1].)

If the above definition holds, we say that R is a finite computation structure (fcs) of characteristic m. It can easily be shown that if R is an fcs of characteristic m, then there exists a subring S in R which is isomorphic to the integers modulo m (Z/mZ). Thus the finite computation structure concept encompasses the class of all modular rings of integers.
Examples:

1) Z/mZ for all integers m.
2) (Z/mZ)[x1,x2,...,xn] for all m and all n.
3) (Z/mZ)**n for all m and all n, where multiplication is component multiplication.
4) (Z/mZ)**n for all m and all n, where multiplication is convolution of n-tuples.
5) GF(p**n) (field of p**n elements) for all primes p and all integers n > 0.

Section 4. Characterization of Modular Rings of Integers

In order to characterize the class of finite computation structures vis-a-vis the FFT, it is first necessary to consider the case of modular rings of integers inasmuch as one of these rings is embedded in every fcs. The goal of this section is to characterize those modular rings of integers which support a K-point FFT. In order to do this, we will draw upon work down by Pollard [11]. In his work, Pollard puts forth necessary conditions for the support of FFT's in modular rings of integers (Theorem A). The method of this section is to prove the converse of Pollard's result (Theorem B), eliminate a case untouched by Pollard (Theorem C), and finally, remove unneeded hypotheses from the resulting equivalence (Theorem D). For the proofs given in this section, the author assumes the reader to have basic understanding of elementary number theory (as in Grosswald [6]) and elementary group theory (as in Birkhoff and Mac-Lane [2]).

Note: In the remainder of the paper we will use the following notational conveniences:

Printed	Written	Meaning
pi	p_i	p sub i, a prime number
ei	e_i	e sub i, a positive integer
pi**ei	$p_i^{e_i}$	p sub i to the e sub i power
Zm	$\mathbb{Z}/m\mathbb{Z}$	The ring of integers modulo m
Zpi**ei	$\mathbb{Z}/p_i^{e_i}\mathbb{Z}$	The ring of integers modulo the ei-th power of the prime pi
Z(m)	$\mathbb{Z}(m)$	The multiplicative group of Zm
Z(pi**ei)	$\mathbb{Z}(p_i^{e_i})$	The multiplicative group of Zpi**ei
ø(m)	$\varphi(m)$	phi of m, the Euler phi-function
wK	ω_K	K-th root of unity

Theorem A: Pollard's theorem. Let m be odd and

$$m = \prod_{i=1}^{r} p_i^{e_i}.$$

If K divides pi-1 for every prime pi dividing m, and if there exists an element wK in Z(m) such that the order of wK in Z(pi**ei) is precisely K for all i, then the modular ring Zm will support a K-point FFT.

Proof: In order to prove this result, we go back to the requirements for K-point FFT support.

(S1) Since K divides each pi-1 for all i, then K and pi are relatively prime for all i. This implies that K is relatively prime to the powers of the pi's and also to the product of the powers of the pi's. Hence, K is relatively prime to m. This implies that K possesses an inverse in Zm.

(S2) By hypothesis, there is an element wK of order K for each Zpi**ei. Then, this element also has order K within Zm.

(S3) The case for l=0 is trivial. The proof for $l \neq 0$ depends heavily on:

Lemma A: Assume the above hypothesis with the additional assumption that m=p**e for some prime p. Then Zm supports a K-point FFT.

Proof of Lemma:

(S1) K divides p-1 and thus, K and p are relatively prime. As a result, K has an inverse in Zp**e.

(S2) By hypothesis, there exists an element wK of order K in Zp**e.

(S3) Again, the case l = 0 is trivial, so we assume l is non-zero. Consider now the expressions for S"sub l". We know that wK**Kl=S"sub l" (wK-1). Clearly, the left hand side of the above equation is zero as wK is a K-th root of unity. We need only show that S"sub l" = 0 (modulo p**e). We can do this by showing that wK-1≠0 (modulo p) for then p**e would divide S"sub l". Now, if wK = 1

(modulo p) then (wK,p)=1 and hence wK would be an element of the subgroup {w in Zp**e such that (w,p)=1} of Z(p**e). This subgroup has order p**(e-1) and Z(p**e) has order (p-1)p**(e-1). But wK is also an element of the cyclic subgroup of Z(p**e) of order K consisting of all the powers of wK. Hence, wK is a common element of two subgroups of Z(p**e) having relatively prime orders, hence the identity. Thus, wK = 1 (modulo p**e). Contradiction. Thus, wK ≠ 1 (modulo p) and S"sub 1" = 0 (modulo p**e).

QED for Lemma.

To continue with the proof of the Theorem, we now let m = prod(pi**ei,i,1,r) where the pi are distinct primes. By Iemma A, we know that Zpi**ei will support K-point FFT's for each i. In particular, S"sub 1" = 0 (mod pi**ei) for each i. By using the Chinese Remainder Algorithm (see Lipson [9] for an excellent discussion of the various Chinese Remainder Algorithms) on the relatively prime moduli pi**ei, we know that S"sub 1" = 0 (modulo prod(pi**ei,i,1,r)); i.e., (modulo m). Thus the three conditions are satisfied and Zm supports K-point FFT's.

QED.

The next Theorem presents the converse to Theorem A and as such characterizes completely the odd numbers which can support K-point FFT's .

Theorem B: If Zm supports K-point FFT's and m = prod(pi**ei,i,1,r), m odd, then K divides pi-1 for all i and there exists an element wK in Zm such that wK is of order K in Zpi**ei for all i.

Proof: Since Zm supports K-point FFT's, then by S1, K has an inverse in Zm and hence K and m are relatively prime. It follows that K and pi are relatively prime for each i. Thus, K does not divide pi for all i. Next we can show that the map

$$\psi : Zm \longrightarrow \prod_{i=1}^{r} Zpi^{**}ei$$

given by $\psi(x)$ = (x mod p1**e1, x mod p2**e2, .. ., x mod pr**er)) is a ring isomorphism and thus induces a group isomorphism between Z(m) and $\prod$Z(pi**ei). First note that the order of Z(m) is

$$\varphi(m) = \varphi\left(\prod_{i=1}^{r} p_i^{e_i}\right) = \prod_{i=1}^{r} \varphi(p_i^{e_i}) = \prod_{i=1}^{r} (p_i-1)p_i^{e_i-1}$$

whereas the order of Z(pi**ei) is given by

$$\varphi(p_i^{e_i}) = (p_i-1)p_i^{e_i-1}$$

We know that if wK has order K in Z(m), then K must divide the order of Z(m). Since K does not divide any pi, then K divides the product prod(pi-1,i,1,r). However, we now show that K divides each factor pi-1. By the 3rd requirement for K-point FFT support (S3), we are guaranteed that S"sub 1" = 0 (modulo m = pi**ei), for all 1 < K-1 and not zero. Since the pi**ei are all relatively prime, then S"sub 1" = 0 (modulo pi**ei) for all i. Now consider the order of wK in Z(pi**ei), say K1. Clearly, K1 divides K. If K1 does not equal K then S"sub K1" = 1+wK**K1+ wK**2K1+...=1 +1+1...=K (modulo pi**ei), since the order of wK is K1. But K and pi**ei are relatively prime for all pi and hence K ≠ 0 (modulo pi**ei). We are then left with the conclusion that if K1 ≠ K, then S"sub K1" ≠ 0 (mod pi**ei), which is a contradiction. Thus, wK has order K in each Z(pi**ei). Thus, K divides the order of the group, i.e., (pi-1)pi**(ei-1). Since K and pi are relatively prime, then K divides pi-1 for every i.

QED.

Having finished categorizing completely the case of odd moduli, we consider now the possiblity of even moduli supporting K-point FFT's. This possibility is discarded by the following theorem.

Theorem C: No even modulus can support an FFT.

Proof: We assume here that K is non-trivial; i.e., K > 1. In order to support a K-point FFT with a modulus m which is even, we must have that K possesses an inverse in Zm. This condition is equivalent to saying that K and m must be relatively prime and hence that K must be odd. If there exists an element wK in Zm of order K, where we now write m = prod(pi**ei,i,1,r) with p1=2, then by means of the isomorphism described in Theorem B, the order of wK in Z(2**e1) must divide K. However, since the order of Z(2**e1) is 2**(e1-1), the order of wK in Z(2**e1) can only be even or 1. It can not be even as it must divide K. Thus we are left with the fact that the order of wK in Z(2**e1) must be 1; i.e., wK = 1 (modulo 2**e1). In order to complete our proof we look at the possible cases for m:

Case 1: m= 2**e1.
In this case, wK has order 1 in Zm = Z2**e1 and hence cannot have order K.

Case 2: m = m1 * 2**e1 where m1 is odd.
If we now invoke condition S3 for FFT support, then S"sub 1" must = 0 (modulo m1 * 2**e1). Since m1 and 2**e1 are relatively prime, this implies that S"sub 1" = 0 (modulo 2**e1) for all 1 < K. If we now look at S"sub 1" however, we find that S"sub 1" = 1 + wK + wK**2 + ... = 1 + 1 + 1 + ... (modulo 2**e1) (since wK = 1 (modulo 2**e1)) = K (modulo 2**e1), which is not equal to 0, as K is odd.

Thus, S"sub 1" is not zero and we have a contradiction.

Since both cases yield a contradiction, we have the result that even moduli cannot support FFT's.

QED.

The last theorem in this section combines all the results of this section and provides for the complete characterization of modular rings of integers which support the FFT.

Theorem D: Zm supports K-point FFT's if and only if K divides pi-1 for every prime pi dividing m.

Proof: Using theorems A,B and C, we see that we need only prove the following assertion in order to obtain the above result:
If K divides pi-1 for all primes pi dividing m, then there exists an element wK in Zm of order K in each Z(pi**ei) (and hence in Zm).
The argument proceeds as follows:

1. Every Z(pi**ei) possess primitive roots of unity;
   i.e., elements ri of order the same as Z(pi**ei)
   which is (pi-1)pi**(ei-1). (See Grosswald [6].)

2. The element wi defined by

$$\omega_i \equiv r_i^{\left(\frac{p_i-1}{K}\right)p_i^{e_i-1}} \quad (\text{modulo } p_i^{e_i})$$

   has order K in Z(pi**ei) since K divides pi-1 and order(ri**n) = order(ri)/gcd(n,order(ri)) = K, where

$$n = \left(\frac{p_i-1}{K}\right)p_i^{e_i-1}$$

3. The element wK which is the unique solution (modulo m) to the following family of congruences:

   wK = wi (modulo pi**ei) i = 1,...,r

   is an element of order K in Z(pi**ei) for all i and thus of order K in Zm.

Thus we see that if the hypothesis holds, we can always find an element of the desired order. As a result, the hypothesis of existence of K-th roots of unity in the equivalence implied by Thorems A, B and C is redundant.

A final remark concerns the removal of the hypothesis for odd primes from Theorems A and B. Inasmuch as K must divide pi-1 for each i and that K is not 1, then the statement that the pi must

be odd is redundant. With the two removals of restrictions as described above, the equivalence of Theorems A, B and C result in exactly the statement of Theorem D.

QED.

Summary: Utilizing the various theorems presented in this section, we have provided a complete characterization of modular rings of integers supporting the Fast Fourier Transforms.

Examples:
1. Z3 can support only 2-point FFT's (with wK = -1).
2. Similarly, Z3**e can only support 2-point FFT's for all e.
3. 8-point FFT's can be performed in Zm for any m of the form prod((8ci+1)**ei,i,1,r) for arbitrary r and ci, where 8ci + 1 is prime.
   e.g., 17**e, 33**e', 17**e * 33**e'.

Section 5: Extension to Finite Computation Structures

As we have seen in section 4, only certain modular rings will support K-point FFT's. We now extend this result to include some of the finite computation structures.

Theorem: If R is a finite computation structure of characteristic m, then R supports a K-point FFT if K divides p-1 for every prime p dividing m.

Proof: Let K divide p-1 for all primes p dividing m. Then by Theorem D we know that Z/mZ supports a K-point FFT. As a result, the requirements S1, S2 and S3 of section 2 hold in Z/mZ. Since R is an fcs of characteristic m, then there exists a subring S of R isomorphic to Z/mZ. Because all of the requirements for support of an FFT involve only ring operations, then any isomorphic copy of Z/mZ will satisfy the support requirements. Thus S supports K-point FFT's. However, the definition of support is essential and thus R also supports K-point FFT's.

QED.

Note: If σ:Z/mZ ——> R is the isomorphism onto a subring of R, then σ(wK) is a K-th root of unity in R. Thus, knowledge of modular K-th roots of unity will be sufficient to compute FFT's in R.

Section 6: Applications

The results presented have been applied to the problems of computing products and powers of symbolic multivariate polynomials over the integers (see [3] and [4]). The following brief example examines the application of the FFT in a finite computation structure to the computation of products of polynomials.

Let f and g be univariate polynomials over some coefficient ring R, with the degree of f = m and the degree of g = n. We can thus write:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m$$

$$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n .$$

The product polynomial h(x) = f(x)*g(x) can then be written as

$$h(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{m+n} x^{m+n},$$

where the coefficients ci are computed by

$$c_j = \sum_{i=0}^{j} a_i b_{j-i} .$$

If we set K = m+n+1 and form 2 K-sequences

$$A = (a_0, a_1, \cdots, a_m, 0, \cdots, 0)$$

$$B = (b_0, b_1, \cdots, b_m, 0, \cdots, 0),$$

then the K-sequence C given by

$$C = (c_0, c_1, \cdots, c_{m+n})$$

is precisely the convolution of A and B, as defined in Section 2. As a result of this observation, if the coefficient ring R supports K-point FFT's, the the product polynomial, h(x) can be computed using FFT's as follows:

1) Form the 2 K-sequences A and B
2) Apply a K-point FFT to each sequence, yielding Â and B̂
3) Multiply Â and B̂ component- wise, yielding in Ĉ.
4) Apply the inverse K-point FFT to obtain C, which is the sequence of coefficients of the product polynomial h.

In particular, if the coefficient ring is the integer, we cannot perform FFT's as there are no roots of unity other than 1 and -1. However, if the largest coefficient (in absolute value) in A, B or C is bounded by M, then we can embed f(x) and g(x) in the polynomial ring Zm[x], where m > 2M and Zm supports K-point

FFT's. Then, the application of the 4 steps mentioned above will compute the product

$$\bar{h}(x) \equiv f(x)\, g(x) \quad (\text{modulo } m)$$

However, since the maximum coefficient is less than m/2, then $h(x) = f(x)g(x)$ and we are finished.
Similarly, if the coefficient ring $R = Z[y]$ (i.e., f and g are bivariate polynomials in x and y over the integers), we can embed f and g in $Zm[x,y]$ where m is sufficiently large and $Zr[y]$ supports K-point FFT's. Again, application of the 4 steps given above will yield a polynomial

$$\bar{h}(x,y) \equiv f(x,y)\, g(x,y) \quad (\text{modulo } m),$$

but since m is chosen appropriately, $h(x,y)$ actually equals $f(x,y)g(x,y)$.
The computation of powers of polynomials proceeds in an *analogous* manner. Studies performed on these two computational problems have indicated that the FFT methods provide significant improvement in the efficiency of these algorithms for a large class of polynomials. (See Bonneau [3] [4]).

Section 7: Summary

This paper has presented several results relating modular arithmetic schemes and the Fast Fourier Transform. In particular, the classes of modular rings of integers in which the FFT may be computed is completely characterized by the prime decomposition of the modulus. Also, an extension of this result for computation structures similar to modular rings of integers yields a sufficiency hypothesis for the computation of FFT.

Further research in this area might be motivated by the desire to find necessary and sufficient conditions for FFT support in finite computation structures or in general rings. As an example, Nicholson [10], using the definition of FFT to be a transformation which takes "convolution-product" rings into "component-product" rings, provides the result that FFT's are supported in division rings (i.e., rings with no zero divisors) iff the ring contains a particular primitive root of unity. It would be most desirable to extend this type of result to a larger class of rings.

References

[1] Albert. Fundamental Concepts of Higher Algebra. University of chicago Press. 1956.

[2] Birkhoff & Mac Lane. A Survey of Modern Algebra. Third edition. MacMillan Co. 1965.

[3] Bonneau. "Polynomial Multiplication and The Fast Fourier Transform." Department of Mathematics, Mass. Institute of Technology, Cambridge, Mass. 1973. (In preparation)

[4] ———. "Polynomial Exponentiation: The Fast Fourier Transform Revisited", Department of Mathematics, Mass. Institute of Technology, Cambridge, Mass. 1973. (In preparation)

[5] Cooley & Tukey. "An Algorithm for the Machine Calculation of Complex Fourier Series." Mathematics of Computation, vol. 19, April 1965. pp. 297-301.

[6] Grosswald. Topics from the Theory of Numbers. Macmillan Company, New York. 1966. Chapter 4.

[7] Knuth. The Art of Computer Programming --Errata et Addenda. Computer Science Department, Stanford University. Jan., 1971. pp. 21-26.

[8] Lang. Algebra. Addison-Wesley Co., Reading, Mass. 1965.

[9] Lipson. "Chinese Remainder and Interpolation Algorithms," Proc. of Second Symposium on Symbolic Algebraic Manipulation, March 1971.

[10] Nicholson. "Algebraic Theory of Finite Fourier Transforms." Journal of Computer and System Sciences, vol. 5, 1971. pp. 524 - 547.

[11] Pollard. "The Fast Fourier Transform in a Finite Field." Mathematics of Computation, vol. 25, number 114, April, 1971. pp. 365 - 374.

[12] Schonhage & Strassen. "Fast Multiplication of Large Numbers," to appear in Computing.